Appendix B
Glossary

The IATF uses Information Assurance terms defined in National Security Telecommunication and Information Systems Security Instruction (NSTISSI) No. 4009, National Information Systems Security (INFOSEC) Glossary. This document can be obtained from The Committee on National Security Systems (CNSS) website (http://www.nstissc.gov/Assets/pdf/4009.pdf). Note, the CNSS was formally known as National Security Telecommunications and Information Systems Security Committee. This glossary defines terminology not available in the NSTISSI No. 4009 and may further expand upon terminology from the NSTISSI No. 4009.

Advanced Mobile Phone Service (AMPS)

The standard system for analog cellular telephone service in the U.S. AMPS allocates frequency ranges within the 800 – 900 MHz spectrum to cellular telephones. Signals cover an area called a cell. Signals are passed into adjacent cells as the user moves to another cell. The analog service of AMPS has been updated to include digital service.

Anonymity

Anonymity is the fact of being anonymous. To provide anonymity, a system will use a security service that prevents the disclosure of information that leads to the identification of the end users. An example is anonymous e-mail that has been directed to a recipient through a third-party server that does not identify the originator of the message.

Application-Level Firewall

A firewall system in which service is provided by processes that maintain complete TCP connection state and sequencing; application level firewalls often re-address traffic so that outgoing traffic appears to have originated from the firewall, rather than the internal host. In contrast to packet filtering firewalls, this firewall must have knowledge of the application data transfer protocol and often has rules about what may be transmitted and what may not.

Application Program Interface (API)

An application program interface (API) is the specific method prescribed by a computer operating system or by an application program by which a programmer writing an application program can make requests of the operating system or another application. An API can be a set of standard software interrupts, calls, and data formats that application programs use to initiate contact with network services, mainframe communications programs, telephone equipment, or program-to-program communications.

Asymmetric Cryptographic Algorithm

An encryption algorithm that requires two different keys for encryption and decryption. These keys are commonly referred to as the public and private keys. Asymmetric algorithms are slower than symmetric algorithms. Furthermore, speed of encryption may be different than the speed of decryption. Generally asymmetric algorithms are either used to exchange symmetric session keys or to digitally sign a message. RSA, RPK, and ECC are examples of asymmetric algorithms.

Asynchronous Transfer Mode (ATM)

ATM (asynchronous transfer mode) Is a fast cell-switched technology based on a fixed-length 53-byte cell. All broadband transmissions (whether audio, data, imaging or video) are divided into a series of cells and routed across an ATM network consisting of links connected by ATM switches (Newton's Telecom Dictionary).

Authentication Header (AH)

An IP device used to provide connectionless integrity and data origin authentication for IP datagrams.

Authentication Token

See token.

CERT

Computer Emergency Response Team – A federally funded research and development center at Carnegie Mellon University. They focus on Internet security vulnerabilities, provide incident response services to sites that have been the victims of attack, publish security alerts, research security and survivability in wide-area-networked computing, and develop site security information. They can be found at http://www.cert.org.

Code Division Multiple Access (CDMA)

CDMA (code-division multiple access) refers to any of several protocols used in wireless communications. As the term implies, CDMA is a form of multiplexing, which allows numerous signals to occupy a single transmission channel, optimizing the use of available bandwidth. The technology is used in ultra-high-frequency (UHF) cellular telephone systems in the 800-MHz and 1.9-GHz bands.

Common Criteria (CC)

The Common Criteria represents the outcome of a series of efforts to develop criteria for evaluation of IT security that are broadly useful within the international community. The Common Criteria is an International Standard (IS 15408) and is a catalog of security functionality and assurance requirements

Compromised Key List (CKL)

A list with the Key Material Identifier (KMID) of every user with compromised key material; key material is compromised when a card and its personal identification number (PIN) are uncontrolled or the user has become a threat to the security of the system.

Computer Intrusion

An incident of unauthorized access to data or an Automated Information System (AIS).

Cryptographic Application Program Interface

A standardized interface to cryptographic functionality. Also see API.

Cryptographic Function

A set of mathematical procedures that provide various algorithms for key generation, random number generation, encryption, decryption, and message digesting.

Customer

The party, or his designee, responsible for the security of designated information. The Customer works closely with an ISSE. Also referred to as the user.

Defense in Depth

An approach for establishing an adequate IA posture whereby (1) IA solutions integrate people, technology and operations; (2) IA solutions are layered within and among IT assets; and (3) IA solutions are selected based on their relative level of robustness. Implementation of this approach recognizes that the highly interactive nature of information systems and enclaves creates a shared risk environment; therefore, the adequate assurance of any single asset is dependent upon the adequate assurance of all interconnecting assets.

Defense-wide Information Assurance Program (DIAP)

The Defense-wide Information Assurance Program, established in January 1998, is the Office of the Secretary of Defense (OSD) mechanism to plan, monitor, coordinate, and integrate IA activities. The DIAP will act as a facilitator for program execution by the Commanders-in-Chief (CINCs), Military Service and Defense Agencies. The DIAP Staff combines functional and programmatic skills for a comprehensive Defense-wide approach to IA. The Staff's continuous development and analysis of IA programs and functions will provide a "big picture" of the Department's IA posture that identifies redundancies, incompatibilities and general shortfalls in IA investments, and deficiencies in resources, functional and operational capabilities.

DoD Information Technology Security Certification and Accreditation Process (DITSCAP)

The DITSCAP (DoDI 5200.40) defines a process that standardizes all activities leading to a successful accreditation. The principal purpose of that process is to protect and secure the entities comprising the DII. Standardizing the process will minimize risks associated with nonstandard security implementations across shared infrastructure and end systems.

Downgrade

The change of a classification label to a lower level without changing the contents of the data. Downgrading occurs only if the content of a file meets the requirements of the sensitivity level of the network for which the data is being delivered.

Eavesdropping

An attack in which an attacker listens to a private communication. The best way to thwart this attack is by making it very difficult for the attacker to make any sense of the communication by encrypting all messages.

Effective Key Length

A measure of strength of a cryptographic algorithm, regardless of actual key length.

Encapsulating Security Payload

This message header is designed of provide a mix of security services that provides confidentiality, data origin authentication, connectionless integrity, an anti-replay service, ad limited traffic flow confidentiality.

Evaluation Assurance Level (EAL)

One of seven increasingly rigorous packages of assurance requirements from CC (Common Criteria (IS 15408)) Part 3. Each numbered package represents a point on the CC's predefined assurance scale. An EAL can be considered a level of confidence in the security functions of an IT (information-technology) product or system.

Frequency Division Multiple Access (FDMA)

FDMA (frequency division multiple access) is the division of the frequency band allocated for wireless cellular telephone communication into 30 channels, each of which can carry a voice conversation or, with digital service, carry digital data. FDMA is a basic technology in the analog Advanced Mobile Phone Service (AMPS), the most widely installed cellular phone system installed in North America. With FDMA, each channel can be assigned to only one user at a time. FDMA is also used in the Total Access Communication System (TACS).

Future Narrow Band Digital Terminal (FNBDT)

FNBDT is an end-to-end secure signaling protocol that will allow establishment of communications interoperability among communications devices that share the same communications capabilities, but are not configured to communicate with each other. FNBDT sets the common configuration. It is a network-independent/transport-independent message layer. FNBDT operates in the Narrow Band portion of the STE spectrum (64 kbps and below).

Global Information Grid (GIG)

It is a globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel.

Global Command and Control system (GCCS)

A comprehensive, worldwide network of systems that provide the NCA, Joint staff, combatant and functional unified commands, services, and defense agencies, Joint Task Forces and their service components, and others with information processing and dissemination capabilities necessary to conduct C2 of forces.

Global Network Information Environment (GNIE)

A composition of all information system technologies used to process, transmit, store, or display DoD information. GNIE has been superceded by Global Information Grid (GIG).

Host-based Security

The technique of securing an individual system from attack; host-based security is operating system and version dependent.

Identification & Authentication (I&A)

Identity of an entity with some level of assurance.

Information Protection Policy

See Security Policy.

Information Systems Security Engineering (ISSE)

The art and science of discovering users' information protection needs and then designing and making information systems, with economy and elegance, so they can safely resist the forces to which they may be subjected.

Information Technology (IT)

The hardware, firmware, and software used as part of the information system to perform DoD information functions. This definition includes computers, telecommunications, automated information systems, and automatic data processing equipment as well as any assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store and/or control data or information.

Insider Attack

An attack originating from inside a protected network.

Internet Control Message Protocol – ICMP

A message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP is used by a device, often a router, to report and acquire a wide range of communications-related information.

Intrusion Detection

Detection of break-ins or break-in attempts either manually or via software expert systems that operate on logs or other information available on the network.

Intrusion Detection System (IDS)

A system that detects and identifies unauthorized or unusual activity on the hosts and networks; this is accomplished by the creation of audit records and checking the audit log against the intrusion thresholds.

Key Management Infrastructure (KMI)

Framework established to issue, maintain, and revoke keys accommodating a variety of security technologies, including the use of software.

Labeling

Process of assigning a representation of the sensitivity of a subject or object

Layered Solution

The judicious placement of security protections and attack countermeasures that can provide an effective set of safeguards that are tailored to the unique needs of a customer's situation.

Local Area Network (LAN)

A limited distance, high-speed data communication system that links computers into a shared system (two to thousands) and is entirely owned by the user. Cabling typically connects these networks.

Mission Needs Statement (MNS)

Describes the mission need or deficiency; identifies threat and projected threat environment

Motivation

The specific technical goal that a potential adversary wants to achieve by an attack, e.g., gain unauthorized access, modify, destroy or prevent authorized access.

Multipurpose Internet Mail Extensions (MIME)

A specification for formatting non-ASCII messages so that they can be sent over the Internet. MIME enables graphics, audio, and video files to be sent and received via the Internet mail system. In addition to e-mail applications, Web browsers also support various MIME types. This enables the browser to display or output files that are not in HTML format. The Internet Engineering Task Force (IETF) defined MIME in 1992.   See also Secure Multipurpose Internet Mail Extensions, S/MIME.

National Information Assurance Partnership (NIAP)

NIAP is a collaboration between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) with a goal to help increase the level of trust consumers have in their information systems and networks through the use of cost-effective security testing, evaluation, and validation programs.

Non-Technical Countermeasure

A security measure, that is not directly part of the network information security processing system, taken to help prevent system vulnerabilities. Non-technical countermeasures encompass a broad range of personnel measures, procedures, and physical facilities that can deter an adversary from exploiting a system.

Open System Interconnection Model (OSI)

A reference model of how messages should be transmitted between any two endpoints of a telecommunication network. The process of communication is divided into seven layers, with each layer adding its own set of special, related functions. The seven layers are the application layer, presentation, session, transport, network, data, and physical layer. Most telecommunication products tend to describe themselves in relation to the OSI model. The OSI model is a single reference view of communication that provides a common ground for education and discussion.

Perimeter-based Security

The technique of securing a network by controlling accesses to all entry and exit points of the network.

Pretty Good Privacy (PGP)

A standard program for securing e-mail and file encryption on the Internet. Its public-key cryptography system allows for the secure transmission of messages and guarantees authenticity by adding digital signatures to messages.

Protection Needs Elicitation (PNE)

Discovering the customer’s prioritized requirements for the protection of information.

Protection Profile (PP)

A Common Criteria term for a set of implementation-independent security requirements for a category of Targets of Evaluation (TOEs) that meet specific consumer needs.

Risk Plane

A graphic technique for depicting the likelihood of particular attacks occurring and the degree of consequence to an operational mission.

Robustness

A characterization of the strength of a security function, mechanism, service, or solution, and the assurance (or confidence) that is implemented and functioning correctly.

Sanitization –

The changing of content information in order to meet the requirements of the sensitivity level of the network to which the information is being sent.

Secret Key

A key used by a symmetric algorithm to encrypt and decrypt data.

Secure Hash

A hash value such that it is computationally infeasible to find a message which corresponds to a given message digest, or to find two different messages which produce the same digest. See FIPS PUB 180 Federal Information Processing Standards Publication 180, dated May 11, 1993.

Secure Multipurpose Internet Mail Extensions—S/MIME

A version of the MIME protocol that supports encrypted messages. S/MIME is based on RSA's public-key encryption technology. See also Multipurpose Internet Mail Extensions, MIME.

Security Management Infrastructure (SMI)

A set of interrelated activities providing security services needed by other security features and mechanisms; SMI functions include registration, ordering, key generation, certificate generation, distribution, accounting, compromise recovery, re-key, destruction, data recovery, and administration.

Security Policy

What security means to the user; a statement of what is meant when claims of security are made. More formally, it is the set of rules and conditions governing the access and use of information. Typically, a security policy will refer to the conventional security services, such as confidentiality, integrity, availability, etc., and perhaps their underlying mechanisms and functions.

Security Target (ST)

A set of security requirements and specifications drawn from the Common Criteria for Information Technology Security Evaluation (CC) to be used as the basis for evaluation of an identified TOE.

Session Key

A temporary symmetric key that is only valid for a short period. Session keys are typically random numbers that can be chosen by either party to a conversation, by both parties in cooperation with one another, or by a trusted third party.

Signature [Digital, Electronic]

A process that operates on a message to assure message source authenticity and integrity, and may be required for source non-repudiation.

Social Engineering

An attack based on deceiving users or administrators at the target site and is typically carried out by an adversary telephoning users or operators and pretending to be an authorized user, to attempt to gain illicit access to systems.

SOCKS

A networking proxy protocol that enables full access across the SOCKS server from one host to another without requiring direct IP reachability. The SOCKS server authenticates and authorizes the requests, establishes a proxy connection, and transmits the data. SOCKS is commonly used as a network firewall that enables hosts behind a SOCKS server to gain full access to the Internet, while preventing unauthorized access from the Internet to the internal hosts.

Strength of Mechanism (SML)

A scale for measuring the relative strength of a security mechanism hierarchically ordered from SML 1 through SML 3.

Symmetric Algorithm

An algorithm where the same key can be used for encryption and decryption.

System Security Authorization Agreement (SSAA)

The SSAA is the formal agreement among the DAA(s), Certifier, user representative, and program manager. It is used throughout the entire DITSCAP to guide actions, document decisions, specify IA requirements, document certification tailoring and level-of-effort, identify potential solutions, and maintain operational systems security.

Tamper

Unauthorized modification that alters the proper functioning of cryptographic or automated information system security equipment in a manner that degrades the security or functionality it provides.

Target of Evaluation (TOE)

A Common Criteria term for an IT product or system and its associated administrator and user guidance documentation that is the subject of a security evaluation.

Technical Countermeasure

A security feature implemented in hardware and/or software, that is incorporated in the network information security processing system.

Technology Gap

A technology that is needed to mitigate a threat at a sufficient level but is not available.

Time Division Multiple Access (TDMA)

A technique to interweave multiple conversations into one transponder so as to appear to get simultaneous conversations.

Token

A token is an object that represents something else, such as another object (either physical or virtual). A security token is a physical device, such as a special smart card, that together with something that a user knows, such as a PIN, will enable authorized access to a computer system or network.

Trusted Operating System

A Trusted Operating System is part of a Trusted Computer Base (TCB) that has been evaluated at an assurance level necessary to protect the data that will be processed. See the definitions for Trusted Computing Base and Trusted Computer System provided below.

Trusted Computing Base (TCB)

"The totality of protection mechanisms within a computer system -- including hardware, firmware, and software -- the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of a trusted computing base to correctly enforce a security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e.g., a user's clearance) related to the security policy." [Page 112 of the Orange Book]

Trusted Computer System

"A system that employs sufficient hardware and software integrity measures to allow its use for processing simultaneously a range of sensitive or classified information." [Page 112 of the Orange Book]

Tunneling Router

A router or system capable of routing traffic by encrypting it and encapsulating it for transmission across an untrusted network, for eventual de-encapsulation and decryption.

Virtual Network Perimeter

A network that appears to be a single protected network behind firewalls, which actually encompasses encrypted virtual links over untrusted networks.

Wide Area Network (WAN)

A data communications network that spans any distance and is usually provided by a public carrier. Users gain access to the two ends of the circuit and the carrier handles the transmission and other services in between.